Cloud Security Services Architecture
Version 1.1 (Feb 23, 2011)

Application
1. Identity/Authentication Service (*) 2. Access Control Service (*) 3. Provisioning Service (Identity & Access Data) 4. Vulnerability Assessment (Code Reviews)
Virtual Machines
1. Virtual Firewall 2. Anti Malware 3. VM Configuration APIs (CPU, Memory, O/S choices) 4. Secure VM Access (VPN, SSH)
Hypervisor
1. Virtual Networking (VLAN, Isolation of Environments – Prod, Dev etc) 2. Console Protection 3. VM Management APIs (Portability, State Control)
Operating System
1. Patch Management 2. Anti Malware
Hardware (Server)
1. (Host-based) IPS/IDS 2.Secure Hardware (e.g., TPM)
Hardware (Storage) & Data
1. Data (at rest) Encryption 2. Key Management 3. Media Protection 4. Data(Block) Level APIs 5. Data Loss Prevention 6. Data Privacy Services (Retention, Destruction) 7. Data Backup and Restore
Network
1. Secure Remote Access (VPN, Radius) 2. Network Segmentation (Firewall, DMZ) 3. Intrusion Prevention/Intrusion Detection (IPS/IDS) 4. Secure Transport Services (TLS, IPSec) 4. Secure Messaging (Encrypted, Signed) 5. Secure Discovery Service (DNSSEC)

(*) These services could reside on the cloud subscriber side or in a different cloud as an independent service (e.g., Identity Provider in a Federation)

Multi-layer Security Services

1. Management/Monitoring
2. Audit (System Access, Transaction, Data)

3. Incident Handling/Response
4. Forensics